Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date filed: 2/29/2008

Name of company covered by this certification: Aroostook Internet

Form 499 Filer ID: 826938

Name of signatory: Eric R. Warren

Title of signatory: IT Manager

I, Eric R. Warren, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI , and what steps companies are taking to protect CPNI.

Please find attached our policies and procedures for protecting our customers' CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed E. R. Warren

Eric R. Warren, IT Manager
Aroostook Internet

STATEMENT OF CORPORATE POLICY

AINOP Phone is committed to honoring the privacy and security of our customer's personal information. We have adopted the protective policies, procedures and enforcement actions described in this manual to protect the privacy of CPNI in accordance with § 222 of the Telecommunications Act of 1996, 47 CFR 64.2001-.2009. The FCC's regulations, 47 CFR 64.2009. This Policy applies to all employees of AINOP Phone and its subsidiaries. Any violation of this policy will subject the employee to the Discipline Policy up to and including immediate discharge. Any employee having knowledge of any violation of the CPNI policy shall promptly report such violation to the appropriate level of management. Senior management (Director Level) of AINOP Phone is responsible for compliance in their area of responsibility.

The duty to protect and ensure the security of AINOP Phone customer's CPNI falls in accordance with the Corporate policies and practices for Confidentiality described in our Employee Handbook and signed by every employee in the "Confidentiality Statement."

New billing department employees will undergo CPNI training upon hire. All billing employees will receive CPNI refresher training on a yearly basis. Upon receiving training, employees will fill out and sign the document included in Appendix 5. This document signifies that they agree that they have received training and understand the material. This document will be kept in the employees' file.

The unauthorized disclosure of CPNI is considered a breach of company policy and warrants the following disciplinary action:

Group 4:
1st Offense: Written Warning or Suspension or Termination (depending on severity of offense)

Any questions regarding compliance with the applicable law and this Manual should be referred to:
Eric Warren, (207) 769-2691 x.10

Any violation of, or departure from, the policies and procedures in this Manual shall be reported immediately to:
Eric Warren, (207) 769-2691 x.10

The policies and processes described within this CPNI manual are new AINOP Phone operating procedures developed to ensure compliance with 47 CFR 64.2001-.2009. They are written to ensure that no use of CPNI is made until a full review of applicable law has occurred.

GENERAL USE OF CPNI

Under federal law, our customers have the right, and we have the duty, to protect the confidentiality of the customers' telecommunications service information. This information includes the type, technical arrangement, quantity, destination, and amount of use of telecommunications services and related billing for these services. This information is called Customer Proprietary Network Information (CPNI). Unless legally compelled to, AINOP Phone and our affiliates will not release CPNI to any outside company.

CPNI includes: where, when, and to whom a customer calls; amount and length of calls a customer makes; services a customer subscribes to (long distance, calling features, etc.); and who the customer's provider is for a given service. Some important points regarding CPNI:

- A Subscriber's published directory information is not CPNI - this includes name, address, and published phone numbers.
- The CPNI rules apply to all types of customer contacts- this includes telephone, in-store/reception area service, as well as the general marketing of services.
- You do not need to seek prior authorization to view a customer's CPNI if you are offering a service of similar status to those the customer already purchases from AINOP Phone. (i.e. Same Bucket)
- You **cannot** market services outside of the customer's "bucket" **without** CPNI approval from the customer - this includes but is not limited to Voice Mail, Inside Wiring Maintenance, Bundled service, Internet, DSL, Cellular, or equipment.
- You must have permission from the customer to use his/her CPNI to market PIC plans/services to them if they are not already PIC'd to AINOP Phone.
- Business customers are exempt in cases where the customer has a dedicated "Account Representative" or a contractual agreement regarding account responsibility with AINOP Phone.
- Opt-In and Opt-Out rules still apply.
- Carriers are permitted to use former customer's CPNI for "Winback" sales attempts only if offering the products/services to which the customer previously subscribed. (Not for new services outside of the former customer-carrier relationship.)
- "Winback" attempts are not permitted until AFTER the PIC change or Port-out request has been completed, and at least 30 days have passed to allow the customer to be moved to another carrier.

For Marketing purposes, AINOP Phone would need to have CPNI approval before we could target a specific group of customers with Internet or Long Distance advertising. For example, AINOP Phone could not send out a DSL advertisement just to customers that currently do not subscribe to our DSL service without their CPNI approval. However, the company could use a mass-marketing approach to advertise to ALL customers in a general area. Service negotiators/representatives are required to ask permission before selling any "out of bucket" service or equipment. This statement is called the Duration of call consent, or "DOCC" statement.

****

Employees who are unsure whether specific information is CPNI, or are in need of assistance with a specific customer contact should ask their Team Leads, or direct Supervisor for procedural clarification. Any violation of this Order will subject the employee to the Corporate Discipline Policy up to and including immediate discharge

.

CUSTOMER SERVICE CPNI REQUIREMENTS AND VERBIAGE

CPNI is account information that details the customer's usage and the prices of their telecommunications services. This includes:

- Current services used/competitors pricing
- Current toll usage data/competitors pricing
- Calling patterns
- Usage data

To keep telecommunication service competition fair, the FCC has mandated that we cannot utilize CPNI information to market/sell any of our products/services without

1st confirming a random account password known only to the "responsible billing party," and 2nd receiving permission from the billing party to "review their records for the purpose of offering additional service options." Also, we must document the customer's account each time the "password" and or "permission" have been given.

The password assigned to the customer's account is required by the FCC to be RANDOM. This means that it cannot be based on "readily available biographical information" (*e.g.*, social security number, mother's maiden name, home address, date of birth) or account information (*e.g.*, account number or any component thereof, amount of last bill, or a phone number associated with that account.) We will have the ability to view the password on a pop-up/alert in QDS.

Establishing an Account Password:

New Customer- Upon the creation of the new account on the AINOP Phone Signup Website, the signup process will now be required to establish an account password, and allow the customer to select a secondary

"non-biographical" security question and answer.

Existing Customer- A randomly generated PIN will be embedded in the comments section of every existing AINOP Phone customer's billing statement. This PIN (now known as the CPIN) will be used to "authenticate" current customers without pre-established account passwords after 12/08/2007. Once we have authenticated the customer via the CPIN, the customer may then set up a password and back up security question with the negotiator. If the customer cannot verify the PIN, other acceptable authentication methods include: (*once Password established, remove CPIN comment)

- Call the account telephone number on record (not CBR #) and upon the owner of the account answering the call, we will then establish an account password, designate the secondary security question and answers within the Subscriber Inquiry, and then handle the customer's service request.
- Call the account telephone number (not CBR #) and leave the CPIN number on the customer's voice mail/answering machine. Upon obtaining the CPIN information, the customer will then need to call customer service for password and security question set-up.
- The customer can come into our billing office and show a valid photo ID, which validates their identity, and allows for full account authorization and disclosure. A password and security question can then be set-up.

For customers with established account passwords, we are to state the following:

CPNI Customer Account Authentication Statement:

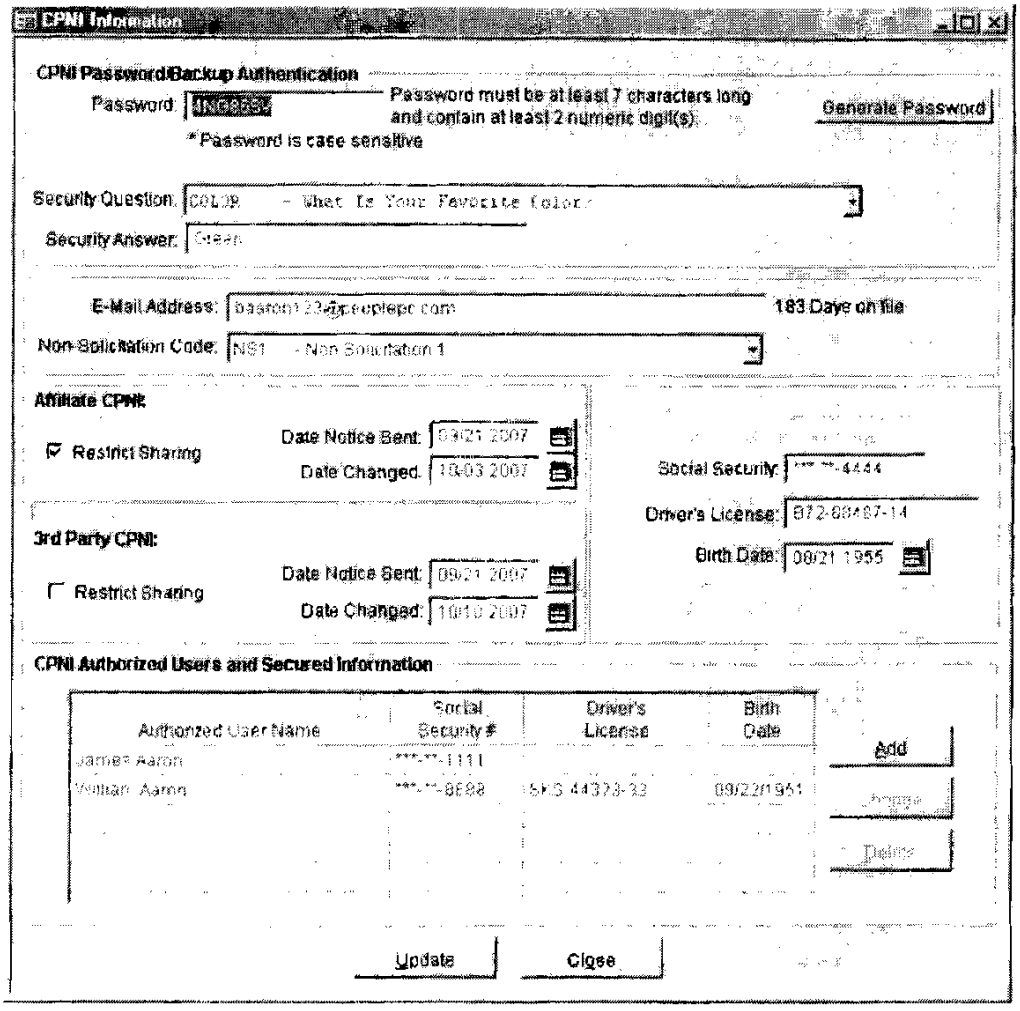
"For security purposes, can you verify your account password?"

If the caller cannot provide the password, we will then ask a previously obtained "non-biographical" security question noted on the customer's account:

Examples of our "non-biographical" security questions: *(also used for EBPP verification)*

- What was the color of your first car?
- What was the name of your first pet?
- What was the name of your favorite fruit?
- Spell your lucky number? (non-numeric)
- What is your favorite musical instrument?

* *Customers with a pre-established password on the AINOP Phone Billing Website will maintain their same password. QDS will automatically populate: Password, SS#, Name, and the DOB fields of the CPNI screen. All email addresses used for CPNI must be entered* ***only*** *on the CPNI window.*



If the caller cannot provide the account password, the answer to the security question, or the CPIN number from their statement, we can do any of the following:

- Call the account telephone number (not CBR #) and upon answering the call, we can advise the customer of their account password, and next handle the customer's service request.
- Send the account password **OR** service request information via e-mail to the customer's e-mail address on record (as long as it has been established for greater than 30 days) **(we cannot send Account info # password together)**
- Send the account password **OR** service request information via U.S. Post office to the customer's billing address on record (as long as it has been established for greater than 30 days)
- The customer can come into our billing office and show a valid photo ID, which validates their identity, and allows for full account authorization and password disclosure.

If the caller accurately provides the password, we then are required

to obtain their permission to "review their records for the purpose of offering additional service options." (See DOCC Authorization Statement)

Documentation of Customer Account Authentication in QDS-

Document Authentication approval in QDS- After the customer has given the appropriate authentication (password or security question), the negotiator will note the information in the comments screen of QDS Subscriber Inquiry. (a new CPNI PSSW comment code will be added)

Example: AA CPNI Password stated by Fred
AAA CPNI Security question answered correctly by Fred

The immediate documentation of a confirmed or a rejected "Authentication" will create a "time stamp" within the Comments screen of when and who we spoke with. This will be of great importance in the event we are ever questioned if the appropriate course of action was performed during any of our customer contacts.

CPNI Authorization Statement: DOCC – "Duration of Call Consent"

Duration of Call Consent (Per Call) Statement or "DOCC" statement is required to obtain a customer's CPNI, to discuss CPE/non-telecommunication services, and/or Telecommunications services in another "bucket" in which the customer does not subscribe. The account information belongs to the customer so the DOCC statement MUST include these key elements:

1) Ask permission to review records
2) State reason why (to possibly make a sales recommendation)

Examples of acceptable Authorization statements include:

- "May I have your name and telephone number, and your permission to access your account and check your service options?"
- "May I have your permission to access your account so I can help you with your request and tell you about our available services?"
- "May I review your account so I can tell you about other features Aroostook Internet is offering?"
- "May I review your records to see what other AINOP Phone services might help you, or you might be interested in?"
- "May I review your records in order to assist you with your inquiry, and also see if there are other services which may help you?"
- "May I have your permission to review your account records for the purpose of offering additional service options?"

Duration of Call Consent (DOCC) allows AINOP Phone to use a customer's CPNI for only the duration of that inbound call. It does not provide AINOP Phone the opportunity to use the customer's CPNI in the future without asking each time for their consent. (Long-Term consent where the DOCC is not needed is considered "General consent" or Opt-In)

Documentation of CPNI Authorization (DOCC) in QDS-

Document DOCC approval in QDS- After the DOCC statement has been provided, and the customer's permission has been obtained to use their CPNI, the negotiator will note the information in the comments screen of QDS Subscriber Inquiry. (a new CPNI DOCC Approved comment code will be added)

Example: AB CPNI DOCC Approved by Fred

Documentation of CPNI Authorization (DOCC) Refusal in QDS-

Document DOCC refusal in QDS- After the DOCC statement has been provided, and the customer has REFUSED to allow us the use of their CPNI, the negotiator will note the information in the comments screen of QDS Subscriber Inquiry. (a new CPNI DOCC Refused comment code will be added)

Example: ABB CPNI DOCC Refused by Fred

*if the customer refuses the DOCC authorization, negotiators may ONLY discuss the specific product or service requested by the customer, within their current usage bucket. NO other "out of bucket" service is to be offered.

DOCC Refusal Contact Documentation in QDS- Included in the **ABB** - CPNI Refusal comment, the negotiator must include a detailed description of the course of action that was taken, what was requested, and by whom .

The documentation sequence of a confirmed or a rejected "Authorization" will create a "time stamp" within the Comments screen of when and who gave us permission to offer the services contained in the order. The "Authorization" comment is required to be entered prior to the creation of the order. This will be of great importance in the event we are ever questioned if the appropriate course of action was performed during any of our customer contacts.

If the caller is a new customer- New customers to AINOP Phone (not an existing AINOP Phone customer requesting additional service) do not require a "DOCC" "Consent statement" to sell any AINOP Phone service or products. Upon the creation of the new account, the AINOP Phone Signup Website will now be required to establish an account password, and allow the customer to select a secondary "non-biographical" security question and provide an answer to that question.

CPNI is not required if offering services directly related to the customer's existing service relationship-

Any carrier may market and/or sell telecommunication services directly related to the customer's current service relationship (i.e. same bucket.) This means that if AINOP Phone is currently providing local service to a customer, we may use CPNI (without customer consent) to sell/offer any additional in the "local service bucket." This includes services such as: Custom Calling Features, listings, additional lines, toll, etc.

If the caller specifically requests "out of bucket" services,

A DOCC statement is not required when a customer specifically asks for or inquires about an "out of bucket service." However, CPNI may only be used for that specific product or service requested by the customer. If any other "out of bucket" service is to be offered, then the negotiator must use the DOCC statement and obtain the customer's approval to continue. A Comment must be entered in QDS subscriber Inquiry that explains the course of action that was taken and when.

Document Customer initiated "out of bucket" requests in QDS- Although the DOCC is not required, it is necessary to document customer initiated requests for "out of bucket" services. The negotiator will note the information in the comments screen of QDS Subscriber Inquiry. (a new CPNI DOCCNA comment code will be added)

Example: ABC CPNI DOCC N/A request for PTN LD initiated by Fred

The FCC requires that AINOP Phone maintain a "retrievable" 1 year record of these notations as to ensure CPNI compliance. All negotiators are required to leave a detailed comment on All accessed QDS accounts.

Reception area and In-Office Customer Contacts:

"In-Office" Customer Service contacts

In-office customer service allows authentication through the presentment of a valid Photo ID prior to the disclosure of CPNI. (Photo ID must be Government Issued) A redesign of the office reception area may be required as to ensure there is proper distance between the customers being serviced, and the customers waiting in line when CPNI is being discussed. In addition to limiting the possibility of eavesdropping, Receptionists must take proper security measures to protect the indirect viewing of their customer's CPNI on their computer monitors or printed transaction receipts.

Documentation of In-Office customer account Authentication in QDS

Document the ID presentment and authentication approval in QDS- After the customer has provided a Government issued photo ID, and appropriate authentication has been determined, the negotiator will note the information in the comments screen of QDS Subscriber Inquiry. (a new CPNI PSSW comment code will be added)

Example: AAAA CPNI ME Lic presented by Fred

Individual duty to protect CPNI

The protection of CPNI carries over to every representatives' work station. We are required to follow the correct shredding practices/recycling procedures outlined within our AINOP Phone Privacy Policy. This policy in general requires, that after internal use, we destroy all credit card/payment information, account service records/statements, printed service orders and anything containing a customer's personal data. In addition to adhering to the required shredding practices, representatives must take proper security measures to protect the indirect viewing of their customer's CPNI on their computer monitors. The Windows security feature will allow the representative to "lock" their computers prior to leaving their work station for any extended time. To regain system access, the representatives will then be required to enter their "sign on password."

CPNI Protection for Online Account Access (EBPP):

CPNI protection for Online Account Access (EBPP)

The Order requires password-protection for online access to CPNI. Because we are prohibited from relying on "readily available biographical information" or "account information" to authenticate a customer's identity before a customer accesses their EBPP (Electronic Bill Pay and Presentment) account, this significantly limits the customer's ability to self-register for EBPP, and our on-line authentication options.

Existing customers with established EBPP accounts and passwords:

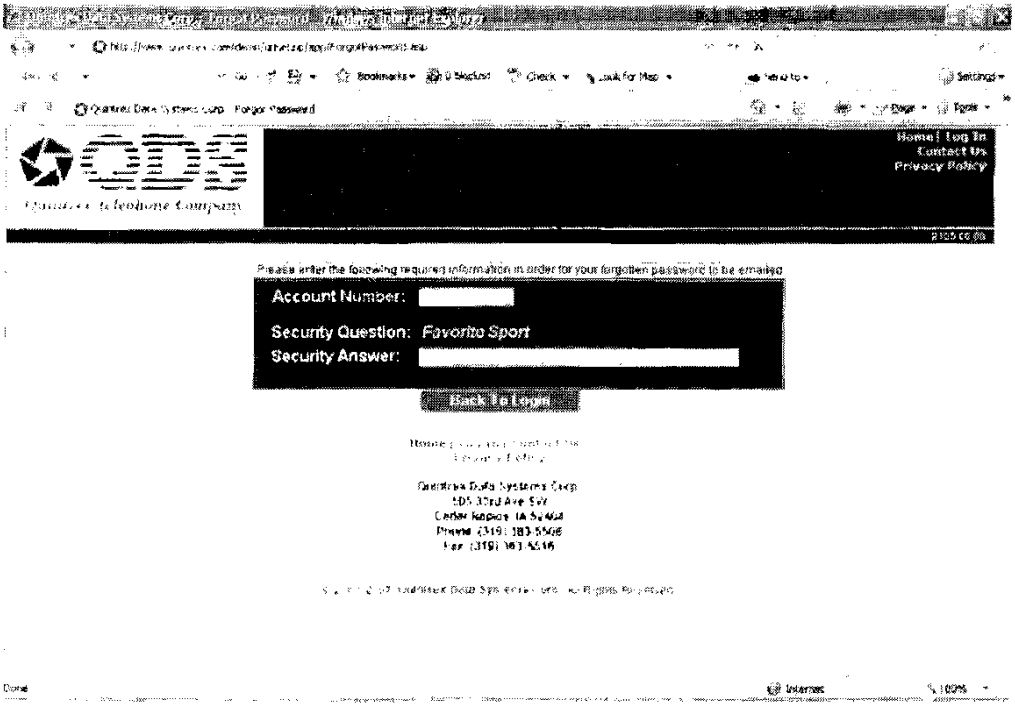
Customers will be allowed to continue to utilize their existing passwords and should experience no problems in completing routine transactions.

Existing customers aspiring to self-register or initialize on-line access to EBPP:

Customers will reach the new account registration screen of our site, and be directed to contact a Customer Service Representative at their local business office to complete the registration. The representative receiving the customer's request to register will need

to follow the FCC's proposed means of authentication-calling a customer at the telephone number of record or confirming the embedded statement CPIN. Once the customer has been authenticated, the CSR will ask the customer to establish a CPNI/On-Line password and back-up authentication question. The customer will now be able to sign up on-line for EBPP.

New customers without established EBPP accounts or passwords:
New customers will, during the AINOP Phone signup process, create a password and select a back-up security question. This will allow the customer to sign up for EBPP.



Notification Process in the event of a CPNI breach:

In the event of a CPNI breach, the FCC CPNI Order mandates the notification of both law enforcement and the affected customers within as designated time frame.

Carriers are required to report CPNI breaches to law enforcement no later than seven business days after a "reasonable determination of a breach," by sending notification through a central reporting facility to the U.S. Secret Service "USSS" and the Federal Bureau of Investigation "FBI"

The disclosure of CPNI breaches to the affected customers are permissible seven days after notification to the USSS and the FBI, providing the law enforcement authorities have not requested continued postponement of the disclosure. If it is determined that there is an "urgent" need for customer notification of the breach as to avoid

"immediate and irreparable harm," we must first consult with the relevant investigative agency, and upon receiving their consent, we may send notification of the breach to the affected customer. Any employee in violation of the CPNI Order, or any employee having knowledge of a violation of the CPNI Order policy shall promptly report such violation to the appropriate level of management. Senior management (Director Level) of AINOP Phone will be responsible for maintaining proper Notification compliance and informing the required divisions of law enforcement through a central reporting facility. The Commission will maintain a link to the reporting facility at http://www.fcc.gov/eb/cpni.

All Carriers are required to maintain for TWO Years, a record of the following:

- **The date that the CPNI breach was discovered**
- **The date notification was sent to the USSS and the FBI**
- **The USSS and FBI response**
- **A detailed description of the CPNI that was breached and the circumstances of the breach**

Employees who are unsure whether specific information is CPNI, or are in need of assistance with a specific customer contact should ask their Team Leads, or direct Supervisor for procedural clarification.

All consumer complaints must be investigated and documented

Any accusation or complaint of unauthorized CPNI disclosure must be reported to the appropriate level of management, and documented in the comments screen of QDS Subscriber Inquiry. **A summary of all consumer complaints received within the year (December 8, 2007- March 1, 2008) regarding the unauthorized release of CPNI, is required to accompany our annual March 1st certification. This includes :**

- **The number of complaints broken down by category (e.g., improper access by employees, by unauthorized individuals, or online)**
- **Information regarding "pretexter" tactics and carriers' protective steps taken.**

Notification Process for Account Changes:

The FCC Order requires that we notify customers immediately when
(a) the customer's password has been changed
(b) customer's response to a "back-up security question" has been changed
(c) online account has been created or changed
(d) address of record has been created or changed

Notification may be sent via voicemail, text message, or an e-mail/letter to the telephone number or address of record. (the notification must NOT reveal the changed account information) QDS has designed a program that will automatically generate a "Notification of Account Changes" spread sheet for any customers with such account changes. (See Appendix for sample Notification letters) A notification will be sent to the AINOP Phone customers' email address. Files of the spread sheets will be maintained for proof of Notification Process compliance.

Suggestions for customers to further guard their information.

.

You can ask AINOP Phone to:

•Deactivate the online access feature if you don't manage your account online.
•Change your telephone number, and request non-published service.
•Set up a non-biographical password for telephone account access.

Four Things for CSRs to Remember:

1. Authenticate every customer, and when necessary, get account Authorization prior to discussing products or services.
2. Authenticate every customer, and when necessary, get account Authorization prior to discussing products or services.
3. Authenticate every customer, and when necessary, get account Authorization prior to discussing products or services.
4. Authenticate every customer, and when necessary, get account Authorization prior to discussing products or services.

!!!!!AUTHENTICATE AND GET AUTHORIZATION!!!!

**********Quick Reference**********

AA = CPNI Password confirmed
AAA= CPNI Security question answered
AAAA=CPNI Photo ID presented
AB= CPNI Authorized DOCC statement
ABB= CPNI Refused DOCC statement
ABC= CPNI N/A DOCC statement
CPIN= Pin Number for CPNI authentication on statements
WELC= Welcome Kit Mailed

APPENDIX 1
SAMPLE CHANGE OF ACCOUNT RESPONSIBILITY LETTER

Telephone Number: XXX-XXX-1234

Dear Customer,

Account Holder responsibility has been changed for the Telephone number listed above.

An Account Holder has full account management authorization including but not limited to the viewing and paying of the monthly statement, as well as various other service and equipment related changes.

If you did not request this change, please contact us immediately at 1-800-752-4330.

Thank you for your immediate attention to this matter.
AINOP Phone

APPENDIX 2
SAMPLE CHANGE OF EBPP ACCOUNT PASSWORD

Telephone Number: XXX-XXX-1234

Dear Customer,

The On-line account password for the Telephone number listed above was changed on 12/9/2007.

Your security is important to us. If you are unaware of this action, please contact us immediately at 1-800-752-4330.

Thank you for your immediate attention to this matter.
AINOP Phone

APPENDIX 3
SAMPLE CHANGE ACCOUNT PASSWORD

Telephone Number: XXX-XXX-1234

Dear Customer,

The account authorization password for the Telephone number listed above was changed on 12/9/2007.

Your security is important to us. If you are unaware of this action, please contact us immediately at 1-800-752-4330.

Thank you for your immediate attention to this matter.
AINOP Phone

APPENDIX 4
SAMPLE CHANGE OF CHANGE OF ADDRESS

Telephone Number: XXX-XXX-1234

Dear Customer,

The On-line account password for the Telephone number listed above was changed on 12/9/2007.

Your security is important to us. If you are unaware of this action, please contact us immediately at 1-800-752-4330.

Thank you for your immediate attention to this matter.
AINOP Phone

APPENDIX 5
Employee Verification of Review of Manual

Employee Name:

Date:

I have reviewed the Company's Customer Proprietary Network Information
Compliance Manual and Operating Procedures and agree to comply with the
procedures set forth therein.

_____

Employee Signature